Cassandra Crossing/ Un tranquillo weekend di TrueCrypt

(319) - La confusione è calata su TrueCrypt, ma non è opportuno farsi prendere dal panico. Le alternative esistono, e sono praticabili.

Cassandra Crossing/ Un tranquillo weekend di TrueCrypt



Figure 1:

(319) - La confusione è calata su TrueCrypt, ma non è opportuno farsi prendere dal panico. Le alternative esistono, e sono praticabili.

9 giugno 2014—C'è probabilmente qualcosa di positivo nel fatto che la scoperta di problemi informatici in un pezzo di software per la privacy conquisti notevole rilevanza sui media, quasi fosse il matrimonio di una stella del rock.

È successo un paio di mesi or sono all'exploit Heartbleed di OpenSSL, è successo la settimana scorsa per l'"affaire" Truecrypt.

Fatto positivo, posto però che non si tratti di una PSYOPS di qualche agenzia triletterata. Come ben sapete i vecchi paranoici come Cassandra si sono sentiti parecchio fessi quando la realtà del Datagate (grazie Edward) ha messo in evidenza che non abbastanza paranoici erano stati, ma semmai creduloni ed ottimisti.

TrueCrypt è un software open source a licenza non completamente libera e ad uso gratuito, realizzato e supportato da un gruppo di programmatori anonimi in rete. Serve a realizzare dischi crittografati, dischi crittografati invisibili e interi sistemi operativi crittografati. La sua funzione più importante è senza dubbio la prima, ma ci torneremo sopra. Cosa è successo dal punto di vista tecnico che giustifichi le notizie dei media?

Il fatto che i sorgenti di TrueCrypt fossero aperti ed esaminabili da chiunque non è, nel caso di TrueCrypt, accompagnato da un processo di sviluppo trasparente e condiviso, come avviene per esempio nel caso di TAILS.

Il fatto che la distribuzione avvenga per lo più in forma binaria, e che non sia reso semplice effettuarsi la ricompilazione direttamente dai sorgenti, insinuano ragionevoli dubbi in chi sia interessato a valutare l'affidabilità di TrueCrypt, particolarmente se si deve utilizzarlo in ambienti critici.

Da molti giorni il sito originale di TrueCrypt è scomparso, sostituito da una pagina molto artigianale, che senza alcuna spiegazione dichiara il software "insicuro", descrive come fare per passare ad "altro" software di crittografia disco "più sicuro", e permette di scaricare una nuova versione di TrueCrypt (7.2) da Sourceforge.Ora, non c'è che da farsi prendere dal panico per fare le cavolate più grosse.

Come prima cosa, **NON installate la versione 7.2 che è infinitamente meno affidabile, ma tenetevi la 7.1a**.

Se aveste già fatto la cavolata di installarla, potete disinstallarla e reinstallare la 7.1a da qui.

Ok, è successo qualcosa, forse semplicemente una lite tra due fazioni del gruppo di sviluppo di TrueCrypt, forse ad uno di loro è arrivata una lettera di quelle di cui non si può parlare ma a cui si deve obbedire, come succede regolarmente in paesi diversamente democratici (tipo Stati Uniti ed Italia) ai provider di connettività e telefonia. Forse mille altre cose.

Ma seguire le indicazioni di cui sopra vi sembra anche solo lontanamente consigliabile?

Dunque, siccome qualcuno, non sapete assolutamente chi, senza darvi alcuna altra spiegazione vi dice che un software a codice sorgente aperto non è più sicuro, voi vi precipitate a scaricare una "nuova versione" di esso di cui non sono disponibili i sorgenti e che chiunque ha potuto pubblicare su Sourceforge? Che sia su Sourceforge non dà infatti nessuna garanzia, se non ai gonzi, che non hanno capito niente dello sviluppo di software, e che considerano il nome del sito come una garanzia.

E poi proseguite dismettendo TrueCrypt? E per di più seguite anche le indicazioni ivi contenute di migrare tutti i vostri dati riservati verso un altro software (BitLocker—nativo del sistema operativo) a sorgenti totalmente chiusi contenuto in un noto sistema operativo, e prodotto da una nota multinazionale dimostratamente ed attivamente implicata nel Datagate?

Non mi addentrerò ulteriormente nel ginepraio di cui sopra, ed invito caldamente chi vi fosse entrato, senz'altra responsabilità che la paura o un momento di ingenuità e distrazione, ad uscirne, tenersi i graffi che si è procurati, conservare la versione TrueCrypt 7.1a se già la usava e buttare la 7.2 se l'avesse installata. Ah, buttate alle ortiche, se vi interessa il parere di Cassandra, anche eventuali drive/folder BitLocker che vi foste nel frattempo costruiti, stando attenti a non perdere i vostri dati.

Ora leggete quanto segue, Troverete notizie positive ed utili.L'unica cosa rilevante dell'"affaire" TrueCrypt è che chi ha fatto l'operazione di cui sopra disponeva della chiave privata con cui il gruppo di sviluppo firmava le nuove versioni del software.

Ma secondo voi conta più il possesso di una chiave o la disponibilità per tutti dei sorgenti di Truecrypt?

"*Nel cyberspazio il software è legge*" diceva Lawrence Lessig, non il possesso di una chiave, che può essere anche frutto di smarrimento, tradimento o coercizione.

Deluderò ora i 24 impazienti lettori chiarendo che nel seguito non troveranno ulteriori analisi dei suddetti accadimenti, ma piuttosto un ragionato elenco di alcuni di questi software, dall'alba della Rete fino ad oggi. Non troveranno infatti istruzioni dettagliatissime su come installarli: questa è probabilmente una delle ultime occasioni che gli verrà offerta per comprendere il mondo della Rete in cui viviamo e cominciare a prendere in mano la propria sicurezza e privacy, uscendo in piccola parte dal Datagate in cui tutti viviamo.

Perderci un po' di tempo è parte necessaria per la sicurezza stessa.Poche parole, scritte da un punto di vista personale, quindi parziale ed ovviamente criticabile, ma con utili indicazioni su usabilità, disponibilità dei sorgenti e possibilità di lavorare da più sistemi operativi.

Crittografare il disco dove si lavora è il minimo comun denominatore di qualsiasi possibilità di riservatezza crittografare l'intero sistema operativo, l'area di swap e di hibernation, od usare sistemi operativi live sono ulteriori opzioni molto efficaci. Fin dai tempi di Pgp era stato prodotto un software che consentiva di criptare i dischi utilizzando gli stessi algoritmi di crittografia forte che Pgp utilizzava. Per limitarsi alla "scena italiana", già il mitico Kriptonite nel lontano 1998 dedicava un intero capitolo al problema dei file system crittati.

Preistoria dell'informatica, al tempo di MS-Dos e Windows NT, tuttavia con software libero e GNU/Linux già ben presenti e consolidati. L'unico software disponibile in ambiente multipiattaforma era a quei tempi un pacchetto open ma commerciale, BestCrypt della finlandese Jetico Inc.. Questa società, nata nei primi anni '90 come produttore di hardware crittografico militare, aveva cominciato a rilasciare utility software gratuite per uso privato.

Nel 1994 rilascia la prima versione di Bestcrypt nella versione GNU/Linux, un open source free, e da allora ha realizzato moltissimi prodotti enterprise e military-grade, ma a ben cercare mantiene ancora versioni free (non possono creare nuovi dischi) ed open source per GNU/Linux (full functional), nonché versioni "portable" per Windows, che permettono di accedere a container già creati senza installazione. Vale la pena di ricordare che il formato dei dischi BestCrypt non è leggibile da altri software simili.

Intorno al 2004 nasce TrueCrypt, il cui gruppo di sviluppo è anonimo (e questo non è necessariamente un problema). Dopo 10 anni di successi, che lo impongono come standard di fatto, avviene un takeover del sito e delle chiavi. A fin di bene o a fin di male ormai non ci interessa.

La disponibilità di tutte le versioni del software e dei sorgenti viene preservata grazie agli sforzi di Steve Gibson e molti altri, mentre un'iniziativa di verifica completa dei codici sorgenti è già da tempo iniziata.

Il mondo del software libero ed aperto non è tuttavia mai stato con le mani in mano, ed ha prodotto, negli ultimi 10 anni alcuni software come Dm-crypt, Cryptsetup e LUKS, che sono diventati standard di fatto per la creazione e l'utilizzo di dischi crittografati.

Come gli altri software FOSS, la loro affidabilità e robustezza non è assoluta, ma equivalente a quella di OpenSSL e di altri pilastri del cyberspazio, ed incomparabilmente superiore a quella di qualsiasi software proprietario e/o a sorgenti chiusi; le verifiche a cui è stato sottoposto sono state infatti incomparabilmente più approfondite.

LUKS è, detto in termini estremamente riassuntivi, un filesystem crittografato modulare, che oltre al suo formato nativo accetta anche quello dei dischi creati da TrueCrypt, anche se non può crearne di nuovi.Contrariamente a TrueCrypt una partizione LUKS ha un header riconoscibile, quindi la sua plausible deniability è inferiore.

Di converso come TrueCrypt possiede i volumi nascosti, e supporta sofisticati schemi di autenticazione come password multiple per aprire lo stesso volume, e password "n su m", cioè esistono

m password, e per aprire il volume ne servono n qualsiasi contemporaneamente.

Il punto dolente di LUKS sono le interfacce grafiche e l'uso cross platform.

Se avete capito qualcosa della vita, ed almeno per le operazioni che ritenete più sensibili usate GNU/Linux (Debian è la scelta di Cassandra) o una live come TAILS, l'utilizzo di volumi LUKS è semplicissimo, perché vengono riconosciuti all'inserimento.

Se siete interessati ad avere un'interfaccia grafica, sempre su GNU/Linux o *nix per gestire i volumi LUKS come da Truecrypt, potete utilizzare ZuluCrypt, pacchetto disponibile a livello sorgente che si compila in maniera abbastanza semplice con solo poco lavoro di interpretazioni delle istruzioni.

Fornisce un'interfaccia simile a quella di TrueCrypt e permette di gestire ambedue i tipi di volume, e quindi non avere nemmeno TrueCrypt installato. E chi usa un diffuso sistema operativo proprietario e non vuole/può smettere? La soluzione minima è continuare ad usare Truecrypt 7.1a.

Una soluzione migliore è quella di cominciare ad utilizzare LUKS: in questo caso l'unico software disponibile è un "abandonware" (ma recente, del 2012, ed ancora reperibile tramite gli Internet Archive) FreeOTFE, che è in grado di utilizzare volumi LUKS, ma i cui driver non sono firmati dal produttore del noto sistema operativo di cui sopra, per cui se possedete una versione 7 o 8 del sistema operativo dovrete riabilitare il caricamento di driver non firmati, utilizzando questa semplice opzione.

A proposito, perché voi, si proprio voi, non ne riprendete lo sviluppo?

Per concludere: nessuna di queste soluzioni è garantita perfetta e sicura, tutte sono frutto di compromessi, ma tutte sono molto meglio di quello che state facendo adesso.

Buon lavoro.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on November 21, 2023.

Canonical link

Exported from Medium on August 27, 2025.